UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,410	07/17/2001	J Kitahara	H-996	2813

7590 07/25/2005

John R Mattingly
Mattingly Stanger & Malur
1800 Diagonal Rd
Suite 370
Alexandria, VA 22314

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,410	KITAHARA, J	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14 and 15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14 and 15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-12 and 14-15 have been considered.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/1/05 has been entered.

Claim Objections

Claim 10 is objected to because of the following informalities: in part a, the word "and" should be inserted between "integrated" and "according". Appropriate correction is required.

Claim 10 is objected to because of the following informalities: the comma after "controller" in part b is unnecessary. Appropriate correction is required.

Claim 10 is objected to because of the following informalities: "from host system" should be "from a host system". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 10 recites the limitation "said single semiconductor chip" in parts a,b, and d. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "said prospecting device" in part a. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2,4-9, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,805,712 in view of Stokes, U.S. Patent No. 6,473,861 in further view of Imai, U.S. Patent No. 5,512,977.

As per claim 1, the applicant describes an information processing apparatus with the following limitations which are met by Davis, Stokes, and Imai:

a) a processing device for performing predetermined processing of information (Davis: Col 8, lines 2-4);

b) a bus for interconnecting said processing device and other component devices of said information processing apparatus (Davis: Col 8, lines 5-6);

c) wherein said processing device is integrated on a single semiconductor chip, internally generates key information, internally encrypts sensitive information inputted from said bus with said generated key information, and outputs said encrypted sensitive information to said bus without outputting key information used for encrypting said sensitive information to said bus (Davis: Col 8, lines 5-22);

d) wherein said processing device newly generates key information each time sensitive information inputted from said bus is encrypted (Imai: Col 2, lines 15-18);

e) wherein said processing device deletes key information in said single semiconductor chip if an abnormality is detected (Stokes: Col 6, lines 56-67);

Davis discloses all the limitations of parts a,b, and c above. Davis does not disclose that the processing device newly generates key information for each encryption process. Imai discloses this limitation in a system which newly generates key information each time sensitive information is input to be encrypted and stored. Combining Imai with Davis allows the hardware agent of Davis' system to generate new key information every time sensitive information is input to the hardware agent. The sensitive data can be, for one example, accounting information (Davis: Col 6, lines 39-41) and encrypting the accounting information in a new key each time the information is received increases protection of the data for at least two reasons: (1) the hacker has less of an opportunity to steal the encryption key because it is newly generated with each encryption process and (2) the hacker would have to steal all the encryption keys (instead of just one encryption key) in order to access all the data.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Imai with those of Davis because doing so provides more protection of the data.

Davis in view of Imai does not disclose that the processing device deletes key information in said single semiconductor chip if an abnormality is detected. Stokes discloses this limitation in a system in which key information is erased if an abnormality, such as opening an enclosure, is detected.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Stokes with those of Davis in view of Imai because doing so prevents key information from being obtained by an unauthorized entry into the system.

As per claim 2, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Stokes in further view of Imai, with the following additional limitation which is also anticipated by Davis:

Wherein said control device comprises an external bus controller for preventing non-encrypted sensitive information from being output onto said bus (Col 5, lines 54-67; Col 6, lines 1-7);

As per claim 4, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Stokes in further view of Imai, with the following additional limitation which is also anticipated by Davis:

Wherein a memory device is provided for storing information encrypted by said control device (Col 8, lines 13-17).

As per claim 5, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Stokes in further view of Imai, with the following additional limitation which is also anticipated by Davis:

Wherein said control device comprises means for decrypting encrypted information at an information write operation (Col 8, lines 13-17);

The applicant should note that the digital certificate at the write operation (storage) comprises means for decrypting encrypted input information.

As per claim 6, the applicant describes the information processing apparatus of claim 5, which is anticipated by Davis in view of Stokes in further view of Imai, with the following additional limitation which is also anticipated by Davis:

a) wherein said information processing apparatus is connected to a different information processing apparatus through a network (Col 10, 11-15);

b) wherein said information processing apparatus decrypts encrypted information which is received from said different information processing apparatus (Col 3, lines 27-30).

The applicant should note that the hardware device can transmit information to another device through a network using a transceiver.

As per claim 7, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Stokes in view of Imai, with the following additional limitation which is also anticipated by Davis:

Wherein a plurality of said processing devices are provided, and cryptographic processing is carried out in each of said processing devices (Col 6, lines 9-32).

As per claim 8, the applicant describes the information processing apparatus of claim 1, which is anticipated by Davis in view of Stokes in view of Imai, with the following additional limitation which is also anticipated by Davis:

Wherein said processing device comprises means for receiving an encrypted program and for carrying out decryption thereof (Col 6, lines 9-32).

As per claim 9, the applicant describes the information processing apparatus of claim 1, which is met by Davis in view of Stokes in view of Imai, with the following limitations which are met by Davis and Stokes:

a) a microprocessor for carrying out said predetermined processing (Davis: 22 of Fig 4);

b) a generator for generating said key information (Davis: 45 of Fig 5; Col 4, line 65);

c) a cryptographic algorithm memory device for storing an algorithm for information cryptographic processing (Davis: 46 of Fig 5; Col 5, lines 11-13);

d) a volatile memory device for storing said generated key information (Davis: 47 of Fig 5; Stokes: Col 7, lines 51-52);

e) a cryptographic processing device for carrying out cryptographic processing with said stored key information according to said algorithm (Davis: 42 of Fig 5; Col 5, lines 1-7);

f) a microprocessor bus for interconnecting said microprocessor, said generator, said cryptographic processing algorithm memory device, said volatile memory device and said cryptographic processing device (Davis: 21 of Figs 4 and 5);

g) wherein a power supply to said volatile memory is stopped so as to delete said key information in said single semiconductor chip if abnormality is detected (Stokes: Col 7, lines 51-52);

Stokes discloses that the keys may be stored in RAM, but he never specifically discloses that the deletion of the keys in RAM is done by cutting the power supply. The examiner takes official notice that it

is well known in the art to delete information stored in RAM by cutting the power to the RAM. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to delete the keys stored in RAM by cutting the power supply because this is a quick, efficient way to delete information stored in RAM.

As per claim 14, the applicant describes the information processing apparatus of claim 1, which is met by Davis in view of Stokes in further view of Imai, with the following limitation which is met by Stokes:

Wherein said abnormality is a disassembly or removal of a case or housing of said processing device (Stokes: Col 4, lines 12-24).

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Stokes in further view of Imai in further view of Hartman, U.S. Patent No. 5,224,166.

As per claim 3, the applicant describes the information processing apparatus of claim 2, which is met by Davis in view of Stokes in further view of Imai, with the following additional limitation which is met by Hartman:

Wherein information not requiring encryption is output onto said bus through said external bus controller (Hartman: Col 3, lines 50-57; Col 6, lines 1-5);

Davis in view of Stokes in further view of Imai disclose all the limitations of claim 2 but fail to disclose the limitation of the above claim. Hartman describes a bus interface which regulates whether information is output in an encrypted or unencrypted form. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the teachings of Hartman with those of Davis in view of Stokes in further view of Imai because it is sometimes necessary for information not requiring encryption to be output to the bus (for example when data is being processed in an already secure area as in Hartman).

Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ote, U.S. Patent No. 6,023,506, in further view of Imai in further view of Stokes in further view of Davis.

As per claim 10, the applicant discloses a disk system controller with the following limitations which are met by Ote, Imai, Stokes, and Davis:

a) wherein said disk system controller, upon receipt of a request for reading out said encrypted information from host system, reads out encrypted filed location information indicating a location of information stored on said magnetic disk from said magnetic disk, internally decrypts said encrypted file location information thus read out in said single semiconductor chip on which said prospecting device is integrated, according to the decrypted file location information, reads out said encrypted information from said magnetic disk (Ote: Col 11, line 50 to Col 13, line 29; Davis: Col 8, lines 11-22).

b) wherein said disk system controller, writes encrypted information into said magnetic disk, updates file location information, internally generates key information in said semiconductor chip, internally encrypts said updated file location information in said single semiconductor chip, and writes said encrypted location information into said magnetic disk without outputting said key information used for encrypting said location information from said single semiconductor chip (Ote: Col 11, line 50 to Col 13, line 29);

c) wherein said disk system controller newly generates key information each time file location information is encrypted (Imai: Col 2, lines 15-18);

d) wherein said disk system controller deletes key information in said single semiconductor chip if an abnormality is detected (Stokes: Col 6, lines 56-67);

Ote discloses a system in which an unencrypted file is selected by a user to be encrypted by an encryption control unit (Col 11, lines 40-42). The encryption control unit encrypts location data associated with the file (Col 11, lines 62-64) and encrypts the unencrypted file (Col 12, lines 3-11). Both the encrypted location information and the encrypted file are stored on the disk.

Ote does not disclose newly generating key information each time file location information is encrypted. Imai discloses a system which newly generates key information each time encryption

processing is performed (Col 2, lines 48-51). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Imai with those of Ote because doing so provides more protection for the data.

Ote in view of Imai does not disclose that the processing device deletes key information in said single semiconductor chip if an abnormality is detected. Stokes discloses this limitation in a system in which key information is erased if an abnormality, such as opening an enclosure, is detected. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Stokes with those of Ote in view of Imai because doing so prevents key information from being obtained by an unauthorized entry into the system.

Ote in view of Imai in further view of Stokes disclose all the limitations of the claim with the exception of the limitation that the encryption control logic is specifically implemented on a semiconductor chip. Davis discloses having the encryption control logic implemented on a semiconductor chip. It would have been obvious to one of ordinary skill in the art at the time the invention to combine the ideas of Davis with those of Ote in view of Imai in further view of Stokes because implementing the encryption control logic in a semiconductor chip makes it easy for the encryption logic to be incorporated in a computing system.

As per claim 11, the applicant describes the disk system controller according to claim 10, which is met by Ote in view of Imai in further view of Stokes in further view of Davis, with the following limitation which is met by Imai:

Wherein said disk system controller is connected to a plurality of magnetic disks (Col 2, lines 3-24).

As per claim 12, the applicant describes the disk system controller according to claim 10, which is met by Ote in view of Imai in further view of Stokes in further view of Davis, with the following limitation which is met by Ote:

a) wherein said disk system is connected to an information processing apparatus (Ote: Col 11, line 50 to Col 13, line 29);

b) wherein said disk system controller reads out encrypted information from said magnetic disk upon receipt of a request therefrom (Ote: Col 11, line 50 to Col 13, line 29).

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Stokes in further view of Imai in further view of Nagai, U.S. Patent No. 6,571,263.

As per claim 15, the applicant describes the information processing apparatus as described in claim 1, which is met by Davis in view of Stokes in further view of Imai, with the following limitation which is met by Nagai:

a) wherein said key information is a random number (Davis: Col 5, lines 3-7);

b) wherein said generator generates said random number based on a signal outputted from a constant voltage diode (Nagai: 8 of Fig 1);

Davis in view of Stokes in further view of Imai discloses all the limitations of claim 1. Davis also discloses the use of random number key generation. However, Davis in view of Stokes in further view of Imai does not disclose the use of a constant voltage diode in the random number generation.

Nagai discloses a random number generator apparatus which includes the use of a zener diode, which is a constant voltage diode. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nagai with those of Davis in view of Stokes and add the use of a constant voltage diode because constant voltage diodes are commonly used in random number generator apparatuses.

Response to Arguments

Applicant's arguments, see Remarks, filed 7/1/05, with respect to the rejection(s)of claim(s) 1 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection has been made.

Conclusion

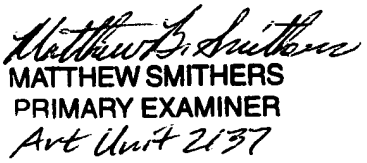
This action is made NON-FINAL.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS



MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137